An Adaptive Image Steganography Technique Using LSB and MSB

Ajanthaa Lakkshmaan,
Puja U. Dharia, Fairy Gandhi

International Research Journal
ISSN 1839-6518
Vol. 3, No. 1, 2013
82800301201302

An Adaptive Image Steganography Technique Using LSB and MSB

Ajanthaa Lakkshmaan,
Puja U. Dharia, Fairy Gandhi

International Research Journal
ISSN 1839-6518
Vol. 3, No. 1, 2013
82800301201302

An Adaptive Image Steganography Technique Using LSB and MSB

IN modern years Steganography is playing a significant role in secure communication. It is a technique of embedding secret information into cover media (image, video, audio and text) such that only the sender and the authoritative receiver can detect the occurrence of hidden information. The two essential properties of Steganography are good visual imperceptibility of the payload which is crucial for security of hidden communication and payload is essential for conveying huge quantity of secret information. Steganography has to satisfy two requirements, one is capability and the other is transparency. Capability means embedding large payload into media. Transparency means an ability to prevent distinction between stego and cover image by statistical analysis. Earlier they have used least significant bit (LSB), the simplest form of Steganography. In LSB method, data is inserted in the least significant bit which leads to a negligible change on the cover image that is not visible to the naked eye. Since this method can be easily cracked, it is more exposed to attacks. In the proposed system we propose Spatial Domain Steganography using 1-Bit Most Significant Bit (MSB) with confused manner.

KEY WORDS: LEAST SIGNIFICANT BIT (LSB), MOST SIGNIFICANT BIT (MSB), STEGANOGRAPHY.

INTRODUCTION

The volatile growth in modern communication like wireless networks and the internet requires security to protect data, resources and to guarantee the authenticity from network based attacks. The two ways of providing security are cryptography and Steganography. The cryptography technique provides solution by scrambling of data with an encryption key. However in this technique the language of the plaintext is known and easily recognized, hence an intruder can suspect encrypted secret information. Steganography is the art and science of writing hidden messages in such a way that no one, except the sender and anticipated recipient, suspects the existence of the message, a form of security through anonymity. Steganography is a term derived from the Greek word Steganos which means covered or secret and graphie means writing or drawing i.e., covered writing. Steganography prevents the intruder from suspecting the secret information in

the cover object. The cover objects are digital files like Images, Video clips, Text, Music, Sound and other digital mediums. The text Steganography is the most difficult technique due to lack of redundant information in a text file compared to an image or a sound file. Digital images are of more concern for Steganography because images contain more redundant information.

STATEMENT OF THE PROBLEM

‘ To study the existing techniques of Steganography and use an enhanced steganographic algorithm to hide the data over an image and to send the stego file to the destination where the retrieving of the secret data is done with improved transparency and capability.’

PURPOSE

The purpose of Steganography is convert communication-to hide the existence of a message from a third person. Steganography differs from cryptography, the art of secret writing, which is proposed to make a message scribbled by a third person but does not hide the presence of the secret communication.

OBJECTIVES OF THE STUDY

This paper has the following objectives:

1. To create a device that can be used to hide data inside a cover image that is decomposed into blocks of 8*8 matrix of equal size.
2. The device should be easy to use, and should use a graphical user interface which effectively hide a message using an image degradation approach, and should be able to retrieve this message afterwards.
3. The device should take into account the original content, to theoretically more effectively hide the message.
4. The device should be able to provide some information as to the effectiveness of the hiding i.e. it should be able to assess the degradation of an image.
5. The procedure should fall under the category of Secret Key Steganography - where without the key the hidden message cannot be retrieved.
6. The device should be able to encrypt the message before embedding it.

APPLICATIONS OF STEGANOGRAPHY

1 Enables secret communication
2 Compliments regular encryption: Hard to break: need to first find the encrypted secret text then it needs to be decrypted.
3 Remarkable use in Military Applications.

EXISTING SYSTEM

Least significant bit (LSB) is the simplest form of Steganography. It is based on inserting data in the least significant bit of pixels, which lead to a minor change on the cover image that is not noticeable to naked eye. Since this method can be easily cracked, it is more susceptible to attacks.

DISADVANTAGES

1 We noticed that in the approach, the time taken for generating the random numbers depends on the size of the key. In our approach it means that it also depends on the cover-image size.
2 Though in LSB embedding methods data is hidden in such a way that the humans do not perceive it, such schemes can be easily destroyed by an opponent such as using lossy compression algorithms or a filtering process.
3 Any process that modifies the values of some pixels, either directly or indirectly may result in degrading of the quality of the original object.
4 LSB method has intense effects on the statistical information of image like. Attackers could be aware of a hidden communication by just checking the Histogram of an image.
5 LSB is extremely susceptible to corruption. That is, the reliability of the hidden message can effortlessly be ruined. All the attacker must do is to randomize the LSBs of the image. The intruder may not even know that it is a stego-image, but such actions would demolish the secret message.

PROPOSED SYSTEM

The development portion of this project focuses on an implementation of the steganographic techniques. This means that the end-product will provide a means for its users to embed a message within an image using steganographic algorithm. This chapter

provides details of the development portion of the project, and also discusses the methodologies and design principles that were considered whilst building the project.

Design Overview

Here we hide the secret information in the spatial domain using LSB and MSB with in increase of the security and capacity. The cover image is decomposed into blocks of 8*8 matrix of the same size. The initial block of cover image is embedded with 8 bits of upper bound and lower bound values required for retrieving payload at the end. The mean of median values and distinction between consecutive pixels is determined to embed payload in 3 bits of Least Significant Bit (LSB) and one bit of MSB.

Architecture diagram

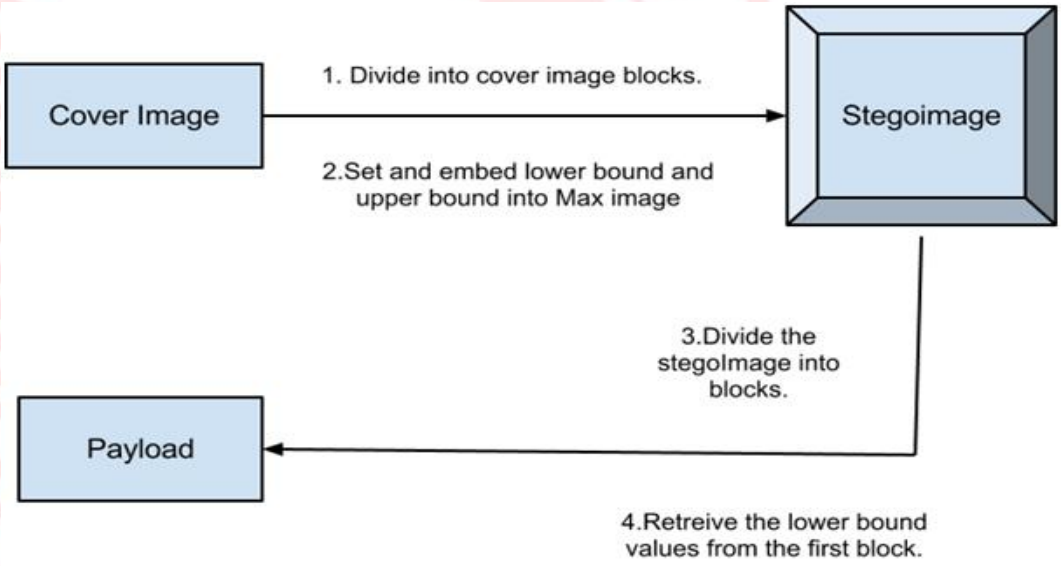

Figure 1: Architecture Diagram of Steganography

Description

1 Cover Image Partition: The cover image of JPG, BMP, TIF, PNG formats with different dimensions are considered. The cover image is divided into 8*8 blocks, to increase security and capacity of payload.

2 Upper and Lower Bound: Set the Upper Bound (UB) and Lower Bound (LB) values with maximum Range (R) of 200 to get optimum PSNR. Embed the bits

of Upper and Lower Bound alternatively in the fifth bit of a pixel in the first block of the cover image using the Equations 1 and 2.

Upper Bound Embedding Position (UBEP)

$$UBEP = p(n,1) \quad (1)$$

Lower Bound Embedding Position (LBEP)

$$LBEP = p(n,5) \quad (2)$$

Where n = 1,2, … 8 (x-coordinate in 8*8 matrix block)

p = pixel intensity value in the cover image.

$$Range, R = UB-LB \quad (3)$$

3 Mean of Median (Me): Consider second block and onwards. Calculate the median value of all columns in each block

$$M = 1/2 \{P(4,n) + P(5,n)\} \quad (4)$$

Where n=1, 2, ….. 8 (y-coordinate in 8*8 matrix block)

Mean of median values in each block is calculated using the

$$Me = 1/8 \{ \sum_{i=1}^{8} M(i) \} \quad (5)$$

4 The difference between the consecutive pixels (Di): Calculate the difference between consecutive pixels from second block of cover image for embedding payload

$$Di = |pi - pi+1| \quad (6)$$

Where i is the index of a pixel in 8*8 matrix block.

5 Di ≤ Me : Compare Di and Me. if Di is less than Me, then embed the payload in both pixels Pi and Pi+1 in the cover image block.

6 Embed Payload: Split each pixel into two equal parts i.e., most part and least part

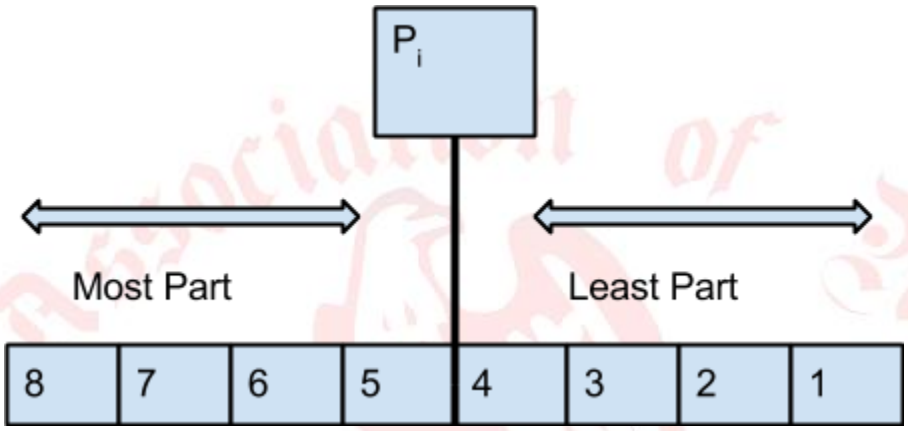

Figure 2: Splitting of pixel

Count the number of ones in the first three bits of most part i.e., 8th, 7th, and 6th positions in the pixel and embed a payload in the pixel.

- **Counter A:** Total number of bits embedded in the 1st position of cover image pixel in case 2 and case 3.
- **Counter B:** Total number of bits embedded in the 5th position of cover image pixel in case 2 and case 3.
- **Counter C:** Number of bits embedded in the 2nd position of cover image pixel in case 2.
- **Counter D:** Number of bits embedded in the 3rd position of cover image pixel in case 3.

Table 1: Embedding payload case

Number of ones in 3-bits of MSB part	Case	Number of bits to embed
0	Case 0	1 bit
1	Case 1	2 bits
2	Case 2	3 bits
3	Case 3	2 bits

- **Case 0:** Embed 1 bit of payload pixel in the 5th position of the cover image pixel.
- **Case 1:** Embed 3 bits of payload pixel in the1st, 2nd and 3rd positions of the cover image pixel.
- **Case 2:** Payload embedding in 5th or 2nd position along with 1st position in a chaotic manner.
- **Case 3:** Payload embedding in 5th or 3rd position along with 1st and 2nd position in a chaotic manner.

Flowchart

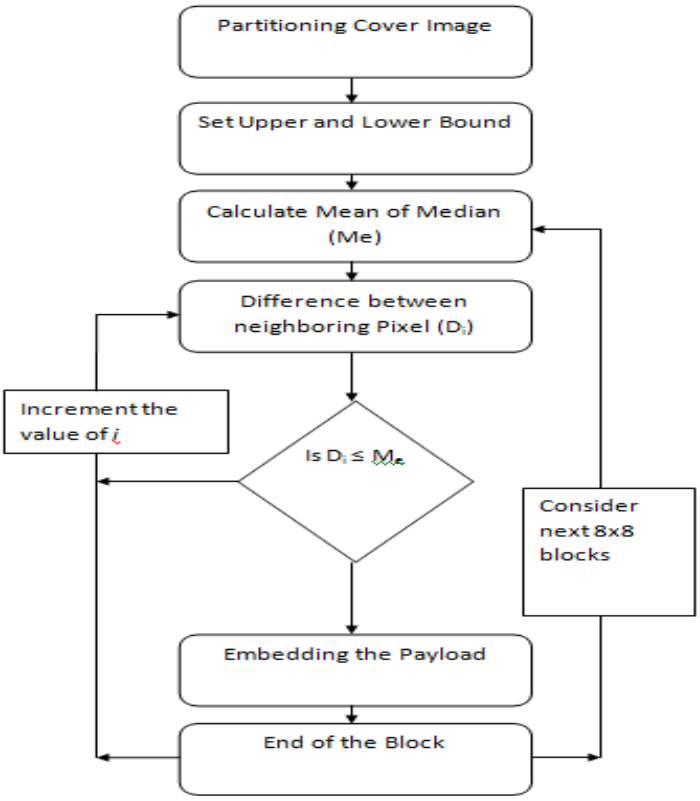

Figure 3: Flowchart of the Algorithm

EVALUATION PARAMETERS

1 Mean Square Error (MSE): It is used to measure the distortion of the image that is the difference of error between the cover image and stego image.

2 Peak to signal noise ratio (PSNR): It is the measure of ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation.

PSNR =10*log10((255)^2/MSE)

3 Capacity: amount of data in a cover image that can be modified without deteriorating the integrity of the cover image. It is represented in bits per pixel.
4 Entropy: It is a measure of security for the system which is considered perfectly secure as Relative Entropy (RE) tends to zero.

RESULTS

Figure 4: Original Image (Desert)

Figure 5: Stego Image (Desert)

Figure 6: Original Image (Penguin)

Figure 7: Stego Image (Penguin)

The original and the stego image of desert and penguin are showing minimal difference after embedding text. This proves that the considered algorithm is better than the simple LSB algorithm.

Performance Analysis

Table 2 : PSNR, RE and Capacity

Combination	PSNR	RE	Capacity in bpp
C.I:- Child.tif P.L:-Baboon.jpg	42.126	0.3122	0.25
C.I:- Eight.tif P.L:-Pears.jpg	45.532	0.3996	0.25
C.I:- Blue Hills.jpg P.L:-Pears.png	41.367	0.0302	0.25

The cover images of Child, Eight, Bluehill and payload images of Baboon, Pears are considered for performance analysis. The PSNR, Relative Entropy (RE) and Capacity are tabulated in the table above.

CONCLUSION AND FUTURE ENHANCEMENTS

In the present world, the data transfers using internet is rapidly growing because its easier as well as faster to transfer the data to destination. So, many individuals and entrepreneurs transfer business documents, vital information using internet. Security is a significant issue while transferring the data using internet because any unauthorized individual can hack the data and make it useless or obtain information un- intended to him. The main intention of the project is to analyze the various Steganography algorithms and develop an enhanced steganographic application algorithm such that it provides good security. In the proposed algorithm the payload bit stream is embedded in both MSB and LSB of the grayscale cover image. The proposed algorithm has high PSNR and security compared to the existing algorithm. It can also be applied on other forms of cover media. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal password. Therefore the data cannot be destroyed easily by an unauthorized person.

In future the same technique can be extended to the transform domain and robustness of the algorithm can be verified. It could also include developing a YASS (Yet Another Steganographic Scheme) and strong encryption algorithms like AES or DES.

REFERENCES

1. Mohammad Reza Abbasy , Bharanidharan Shanmugam, "Enabling Data Hiding for Resource Sharing in Cloud Computing Environments Based on DNA Sequences", 2011.
2. Chen, W.-J., Chang, C.-C., Le, T.H.N.: 'High payload Steganography mechanism using hybrid edge detector', 2010.
3. Pevny, T., Bas, P., Fridrich, J.: 'Steganalysis by subtractive pixel adjacency matrix', 2010.
4. Amirthanjan, R. Akila, R & Deepika chowdavarapu, 'A Comparative Analysis of Image Steganography', 2010.
5. Bandyopadhyay, S.K., 2010. An Alternative Approach of Steganography Using Reference Image. International Journal of Advancements in Technology, 1(1), pp.05-11.
6. Yang, C.-H.: 'Inverted pattern approach to improve image quality of information hiding by LSB substitution', 2008.

– END –

International Association of Research Scholars

IARS

Certificate of Recognition

This certificate is awarded to

Ajanthaa Lakkshmaan

in recognition of his contribution

"An Adaptive Image Steganography Technique Using LSB and MSB"

to Vol. 03, No. 01, 2013 *of*

IARS International Research Journal

Manal Jawdy

.....

Chief Managing Editor

IARS International Research Journal 08 FEB 2013